## AMENDMENTS TO THE CLAIMS

**This listing of claims will replace all prior versions and listings of claims in the application:**

**LISTING OF CLAIMS:**

1. (currently amended): A mobile terminal capable of identifying an authorized user, when ~~a user connects~~ a detachable memory medium is connected to the mobile terminal, based on identification (ID) information stored in the memory medium, comprising:

memory area creating means for dynamically creating a memory area in the mobile terminal, allocated for the ~~which is unique to each~~ authorized user and identified by~~, in association with~~ the ID information of the authorized user;

encrypting means for reading out the ID information from the memory medium connected to the mobile terminal, and encrypting personal contents fed to the mobile terminal on the basis of the ID information;

storing means for storing the encrypted personal contents in ~~a specific~~the allocated memory area ~~associated with~~identified by the ID information; and

decrypting means for reading out the ID information from the memory medium connected to the mobile terminal, and decrypting, based on the ID information, the personal contents encrypted and stored in the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information, thereby rendering the personal contents accessible to the user.

2. (currently amended): The mobile terminal according to Claim 1, wherein:

said memory area creating means automatically creates, in response to the memory medium being connected to the mobile terminal, the ~~specific~~ allocated memory area ~~in association with~~ identified by the ID information stored in the memory medium.

3. (currently amended): The mobile terminal according to Claim 2, wherein:

said memory area creating means includes means for, ~~when~~ if the memory medium is connected to the mobile terminal, providing a subordinate memory area associated with the ~~specific~~ allocated memory area in accordance with ~~the user's~~an operation by the user.

4. (currently amended): The mobile terminal according to Claim 1, further comprising:

information sharing means which allows the ~~users~~ user ~~at least~~ either to write contents into a common memory area, which is shared by a plurality of authorized users, or to gain access to contents stored in the common memory area.

5. (currently amended): The mobile terminal according to Claim 4, further comprising:

operation means for, ~~when~~ if the memory medium is connected ~~by the user~~ to the mobile terminal and the personal contents is accessible by the user, at least either ~~coping~~ copying or transferring the personal contents to the common memory area in accordance with ~~the user's~~an operation by the user.

6. (currently amended): The mobile terminal according to Claim 4, further comprising:

operation means for, ~~when~~ if the memory medium is connected ~~by the user~~ to the mobile terminal and the personal contents is accessible by the user, at least either ~~coping~~ copying or transferring information stored at the common memory area to the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information in accordance with ~~the user's~~an operation by the user.

7. (currently amended): The mobile terminal according to Claim 1, wherein:

said encrypting means generates a cryptographic key based on the ID information read out from the memory medium connected to the mobile terminal, and encrypts personal contents using the cryptographic key.

8. (currently amended): The mobile terminal according to Claim 1, wherein:

said decrypting means generates a cryptographic key on the basis of the ID information read out from the memory medium connected to the mobile terminal, and decrypts the encrypted personal contents stored in the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information by using the cryptographic key.

9. (original): The mobile terminal according to Claim 1, wherein:

the ID information is a subscriber information used for identifying a subscriber who is authorized to receive service to be provided via the mobile terminal, or a serial number uniquely assigned to the mobile terminal.

10. (currently amended): The mobile terminal according to Claim 1, wherein:

said storing means and decrypting means dynamically manage encrypted personal contents as data files having ~~a~~ varied sizes in accordance with file management information which makes it possible to properly manage the association of ID information of individual authorized users with their ~~specific~~ allocated memory areas.

11. (currently amended): The mobile terminal according to Claim 1, wherein:

the mobile terminal is shared by a plurality of users and comprises ~~a fixed specific~~ an allocated memory area uniquely assigned to each of the ~~user~~users;

said storing means, ~~when~~ if the encrypted personal contents of a user is stored in the ~~fixed~~ allocated memory area ~~specifically~~ assigned to the user, attaches a tag on a header portion of the ~~fixed~~ allocated memory area; and

said decrypting means, ~~when~~ if it is required to decrypt the encrypted personal data, determines the ~~fixed~~ allocated memory area specifically assigned to the user by seeking the tag based on the ID information read from the memory medium currently connected to the mobile terminal.

12. (original): The mobile terminal according to Claim 1, wherein:

the memory medium is an IC card based on a common standard.

13. (currently amended): A method for managing information in a mobile terminal comprising a body and a detachable memory medium ~~with the memory medium carrying~~storing identification (ID) information~~ being attached to or detached from the body~~, the method comprising:

if the memory medium is attached to the mobile terminal, reading the ID information from ~~a~~ the memory medium~~ connected to the mobile terminal~~;

dynamically creating a memory area in the mobile terminal, allocated for an authorized user and identified by the ID information read from the memory medium;

encrypting personal contents fed to the mobile terminal on the basis of the ID information, and storing the encrypted personal contents in ~~a specific~~an allocated memory area ~~associated with~~identified by the ID information; and

~~reading out ID information from the memory medium when the memory medium is connected by a user to the mobile terminal; and~~

decrypting, when the encrypted personal contents is stored in ~~a specific~~the allocated memory area identified by ~~associated with~~ the ID information, the encrypted personal contents based on the ID information, thereby rendering the personal contents accessible to the user.

14. (currently amended): The information management method according to Claim 13, ~~further comprising:~~

~~reading, in response to the memory medium being connected to the mobile terminal, the ID information from the memory medium; and~~wherein the dynamically creating the allocated memory area comprises:

automatically creating the ~~specific~~ allocated memory area ~~in association with~~identified by the ID information.

15. (currently amended): The information management method according to Claim 13, wherein:

in said encrypting, a cryptographic key is generated on the basis of the ID information read out from ~~a~~ the memory medium connected to the mobile terminal, and the personal contents fed to the mobile terminal is encrypted by using the cryptographic key.

16. (currently amended): The information management method according to Claim 14, wherein:

in said encrypting, a cryptographic key is generated on the basis of the ID information read out from ~~a~~ the memory medium connected to the mobile terminal, and the personal contents fed to the mobile terminal is encrypted by using the cryptographic key.

17. (currently amended): The information management method according to Claim 13, wherein:

in said decrypting, a cryptographic key is generated on the basis of the ID information read out from ~~a~~ the memory medium connected to the mobile terminal, and the encrypted personal contents stored in the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information is decrypted by using the cryptographic key.

18. (currently amended): The information management method according to Claim 14, wherein:

in said decrypting, a cryptographic key is generated on the basis of the ID information read out from ~~a~~ the memory medium connected to the mobile terminal, and the encrypted personal contents stored in the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information is decrypted by using the cryptographic key.

19. (original): The information management method according to Claim 13, wherein:

the ID information is a subscriber information used for identifying a subscriber who is authorized to receive service to be provided via the mobile terminal, or a serial number uniquely assigned to the mobile terminal.

20. (currently amended): ~~A computer program for controlling an operation of a mobile terminal capable of identifying~~A computer-readable medium embodying a program, said program causing a mobile terminal to identify an unauthorized user, when a detachable memory medium is connected to the ~~motile~~ mobile terminal, ~~an authorized user~~ based on ID information stored in the memory medium, by implementing the computer program in the mobile terminal, the mobile terminal realizes:

a memory area creating function of dynamically creating a memory area, in the mobile terminal allocated for the ~~which is unique to each~~ authorized user, ~~in association with~~and identified by the ID information of the authorized user;

an encrypting function of reading out the ID information from the memory medium connected to the mobile terminal, and encrypting personal contents fed to the mobile terminal on the basis of the ID information;

a storing function of storing the encrypted personal contents in ~~a specific~~the allocated memory area ~~associated with~~identified by the ID information; and

a decrypting function of reading out the ID information from the memory medium connected to the mobile terminal, and decrypting, based on the ID information, the personal contents encrypted and stored in the ~~specific~~ allocated memory area ~~associated with~~identified by the ID information, thereby rendering the personal contents accessible to the user.